WHAT IS CLAIMED IS:

1. An encryption apparatus for performing public-key-cryptosystem encryption processing, comprising:

public-key-cryptosystem processing means including a register group composed of registers for retaining values for use in arithmetic operations and registers for capturing the results of the arithmetic operations, said public-key-cryptosystem processing means performing public-key-cryptosystem encryption processing; and

hash value generating means for generating a hash value for use in said public-key-cryptosystem processing means,

wherein the register group is also used as at least a register group composed of registers for retaining values for arithmetic operations in said hash value generating means and registers for capturing a resultant hash value, and hardware components are changed in a time-sharing manner in accordance with a processing mode.

2. An encryption apparatus according to claim 1, further comprising common-key-cryptosystem encryption processing means for generating random numbers which are necessary when said public-key-cryptosystem processing means performs encryption processing,

wherein the register group in said public-key-

cryptosystem processing means is also used as a register group in said common-key-cryptosystem processing means which is composed of registers for retaining data and registers for retaining key data.

3. An encryption apparatus according to claim 2, wherein said common-key-cryptosystem encryption processing means performs Data Encryption Standard encryption processing.

4. An encryption apparatus according to claim 1, wherein:

said public-key-cryptosystem processing means includes public-key-cryptosystem-operation core means for performing various types of arithmetic operations in the public-key-cryptosystem encryption processing;

said hash value generating means includes hash-value-operation core means for various types of arithmetic operations in the hash value generation; and

said public-key-cryptosystem-operation core means and said hash-value-operation core means share the same hardware components.

5. An encryption apparatus according to claim 4, wherein:

said public-key-cryptosystem-operation core means includes adding means, and said hash-value-operation core means includes adding means; and

the adding means of said public-key-cryptosystem-operation core means and the adding means of the said hash-value-operation core means share the same hardware components.

6. An encryption apparatus according to claim 1, wherein:

said public-key-cryptosystem-operation core means includes a bus-changeover switch for changing bit width; and

said hash value generating means includes a bus-changeover switch for changing bit width which is also used as the bus-changeover switch of said public-key-cryptosystem processing means.

7. An encryption apparatus according to claim 6, further comprising common-key-cryptosystem processing means which performs common-key-cryptosystem encryption processing for generating random numbers which are necessary for the encryption processing by the public-key-cryptosystem processing means,

wherein said common-key-cryptosystem processing means includes a bus-changeover switch which is also used as the

bus-changeover switch of said public-key-cryptosystem processing means.

8. An encryption apparatus according to claim 1, further comprising storage means for storing the hash value generated by said hash value generating means,

wherein:

said hash value generating means stores the generated hash value at an address used by said public-key-cryptosystem processing means when storing the generated hash value in said storage means; and

said public-key-cryptosystem processing means reads the stored hash value from said storage means.

9. An encryption apparatus according to claim 1, wherein said public-key-cryptosystem processing means performs Elliptic Curve Cryptosystem processing.

10. An encryption apparatus according to claim 1, wherein said hash value generating means performs Secure Hash Algorithm 1 processing.

11. A noncontact integrated circuit card having a communication function, comprising an encryption apparatus according to claim 1 which is built into said noncontact

integrated circuit card.